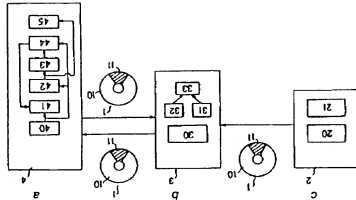


(54) SOFTWARE STORAGE MEDIUM, SOFTWARE READER, AND SOFTWARE MANAGEMENT SYSTEM

- (11) 6-95371 (A) (43) 8.4.1994 (19) JP
 (21) Appl. No. 4-105033 (22) 24.4.1992
 (71) FUJITSU LTD (72) RYOTA AKIYAMA(2)
 (51) Int. Cl. G06F9/06; G09C1/00

PURPOSE: To provide a storage medium which promotes the prevention of the illegal usage of a software spreading on a circulation route, reader of the software of the storage medium, and management system which checks the illegal usage of the software of the storage medium.

CONSTITUTION: A hybrid type storage medium constituted by the combination of a non-reloadable storage area 10 with a reloadable area 11 is prepared as a storage medium 1, the cipher information of the software to be offered is recorded in the non-reloadable storage area 10, and the cipher information of key information for decoding the cipher software and the usable period of time of the software is recorded in the reloadable storage area 11. On the other hand, a reader 4 is constituted to decrease the usable period of time of the storage medium 1 according to the lapse of time, and to inhibit the usage of the software beyond the usable period of time. On the other hand, the management system is constituted to check the illegal usage of the software according to the display value of the number of time of the using period of time of the storage medium 1.



2: origin of output device, 3: destination of repetition device,
 4: user side, b: destination of repetition, c: origin of output

(19)日本国特許庁(J P)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平6-95871

(43)公開日 平成6年(1994)4月8日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	4 5 0 L	9367-5B		
	B	9367-5B		
G 0 9 C 1/00	3 1 0	8837-5L		

審査請求 未請求 請求項の数7(全 13 頁)

(21)出願番号	特願平4-105033	(71)出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中1015番地
(22)出願日	平成4年(1992)4月24日	(72)発明者	秋山 良太 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72)発明者	長谷部 高行 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72)発明者	吉岡 誠 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(74)代理人	弁理士 森田 寛 (外1名)

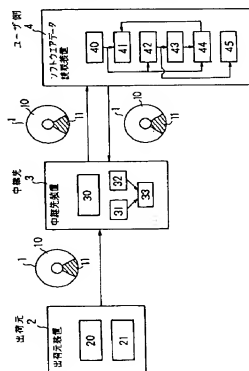
(54)【発明の名称】 ソフトウェア記憶媒体、ソフトウェア読取装置及びソフトウェア管理システム

(57)【要約】

【目的】本発明は、流通経路を流布するソフトウェアの不正使用の防止を促進できる記憶媒体と、その記憶媒体のソフトウェアの読取装置と、その記憶媒体のソフトウェアの不正使用をチェックする管理システムに関する。

【構成】記憶媒体として、書換不可能記憶領域10と書換可能記憶領域11との混成からなる混成型記憶媒体を用意し、この書換不可能記憶領域10に、提供対象のソフトウェアの暗号情報を記録するとともに、この書換可能記憶領域11に、暗号ソフトウェア復号用の鍵情報とソフトウェアの使用可能時間との暗号情報を記録する構成を採り、一方、読取装置は、経過時間に応じて記憶媒体の使用可能時間を減じていくとともに、使用可能時間以上のソフトウェア使用を禁止していく構成を取り、一方、管理システムは、記憶媒体の使用時間回数の表示値に従って、ソフトウェアの不正使用をチェックしていくように構成する。

本発明の原理構成図



(2)

特開平6-95871

【特許請求の範囲】

【請求項1】 流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体であって、ソフトウェア記憶媒体として、書換不可能記憶領域(10)と書換可能記憶領域(11)との構成からなる混成型記憶媒体を用意し、該混成型記憶媒体の書換不可能記憶領域(10)に、提供対象となるソフトウェアの暗号情報を記録する構成を採るとともに、該混成型記憶媒体の書換可能記憶領域(11)に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能時間との暗号情報を、暗号ソフトウェア保護情報として記録する構成を採ることを、

特徴とするソフトウェア記憶媒体。

【請求項2】 請求項1記載のソフトウェア記憶媒体において、ソフトウェアの使用可能時間の初期値が、流通経路途中で記録されるよう構成されることを、

特徴とするソフトウェア記憶媒体。

【請求項3】 請求項1又は2記載のソフトウェア記憶媒体において、暗号ソフトウェア保護情報を多重構成で暗号化していく構成を採るとともに、流通経路途中で、この多重暗号化構成を変更していくよう構成されることを、

特徴とするソフトウェア記憶媒体。

【請求項4】 請求項1、2又は3記載の記録構成を採るソフトウェア記憶媒体に記録される暗号ソフトウェアを読み取るためのソフトウェア読取装置であって、暗号ソフトウェア保護情報を復号することで、暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能時間とを復号する第1の復号手段(40)と、上記第1の復号手段(40)の復号する鍵情報に従って暗号ソフトウェアを復号する第2の復号手段(41)と、上記第1の復号手段(40)の復号する使用可能時間を経過時間に従って減算していくことで新たな使用可能時間を算出する算出手段(42)と、

上記算出手段(42)の算出する新たな使用可能時間に従って、ソフトウェア記憶媒体の記録する暗号ソフトウェア保護情報の使用可能時間を適時更新していく更新手段(43)と、

上記第1の復号手段(40)の復号する使用可能時間が、上記算出手段(42)の算出する使用可能時間のいずれか一方がゼロ値を表示するときには、上記第2の復号手段(41)が復号処理を実行できないように制御する抑止手段(44)とを備えることを、

特徴するソフトウェア読取装置。

【請求項5】 請求項4記載のソフトウェア読取装置において、

使用可能時間の減算値がゼロ値に達するときに新たな使用可能時間となる使用追加時間を設定して、本来の使用可能時間と識別可能となる態様に従いつつ、この新たな

使用可能時間に従ってソフトウェア記憶媒体の記録する暗号ソフトウェア保護情報の使用可能時間を更新する設定手段(45)を備えることを、

特徴するソフトウェア読取装置。

【請求項6】 請求項1、2又は3記載の記録構成を採るソフトウェア記憶媒体に記録されるソフトウェアの使用状態を管理するためのソフトウェア管理システムであって、

流通経路から回収したソフトウェア記憶媒体に記録されるソフトウェアの使用可能時間を集計していくことで、ソフトウェアの使用時間を算出していくよう構成されることを、

特徴とするソフトウェア管理システム。

【請求項7】 請求項6記載のソフトウェア管理システムにおいて、ソフトウェアの使用可能時間の集計を、ソフトウェア記憶媒体の識別番号を単位として実行していくよう構成されることを、

特徴とするソフトウェア管理システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るためのソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするためのソフトウェア管理システムに関する。特に、流通経路を流布するソフトウェアの不正使用の防止を促進できるソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るためのソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするためのソフトウェア管理システムに関する。

【0002】 最近、情報化社会の発達に伴って、コンピュータプログラムや電子出版や娯楽ビデオ等のソフトウェアを、通信ネットワークと連携して、書店等の販売店で販売したり、レンタルビデオ店等のレンタル店で貸し出していくことが行われている。このような流通経路を流布するソフトウェアは、流通段階で、不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複製されたりというように不正使用にさらされることになる。このような不正使用は、ソフトウェア提供者や販売店やレンタル店の利益を著しく害する。これから、流通経路を流布するソフトウェアの不正使用の防止を実現できる新たな仕組みの構築が叫ばれているのである。

【0003】

【従来の技術】 流通経路を介してソフトウェアを貸し出していく場合に、貸し出されるソフトウェアを保護する方法として、従来では、レンタル店による管理でこれを実現するという方法を採用していた

【0004】すなわち、媒体製造メーカーが、ソフトウェアをCD-ROM等の書き換え不可能な不揮発性の記憶媒体に記録する構成を採って、このソフトウェアの記憶媒体をソフトウェア市場に提供していくときにあって、レンタル店は、万引きを防止するために、ソフトウェアの収納ケースのみを陳列棚に並べておいて、ソフトウェアの本体については別の保管場所に管理する構成を採るとともに、持ち逃げを防止するために、ソフトウェアの貸し出し時に、身分証明書等によりユーザの身元を押さえてから貸し出ししていく構成を採る。そして、レンタル料については、貸し出し日と返却日との差より算出して徴収していくという管理構成を採る。

【0005】この管理構成に従って、レンタル店は、ソフトウェアの万引きや持ち逃げを防止しつつ、可能な限りの不正使用の防止を図っているのである。なお、媒体製造メーカーは、ソフトウェアを暗号化して記憶媒体に記録していく構成を採ることがあり、このときには、ユーザは、記憶媒体に記録されるこの暗号ソフトウェアを復号可能とする復号装置を購入することになる。

【0006】【発明が解決しようとする課題】しかしながら、この従来技術に従うソフトウェアの貸し出し方法では、ソフトウェアの不正複写を防止することができないという問題点がある。すなわち、レンタル先以外のユーザが、品質劣化のないソフトウェアを容易に入手できてしまうという問題点がある。また、ソフトウェアの不正横流しを防止することができないという問題点もある。

【0007】また、万引き防止のために、ソフトウェア本体を陳列棚とは別の保管場所に管理することは経済的に得策でないという問題点がある。また、持ち逃げ防止のために、身分証明書等の提示を求めることはユーザの精神的負担を強いることになるという問題点もある。

【0008】このように、従来技術に従っていること、流通経路を流布するソフトウェアの不正使用を有効に防止することができないことから、ソフトウェア提供者の利益が著しく害されるときに、レンタル店の利益が著しく害されることになるという問題点があった。

【0009】本発明はかかる事情に鑑みてなされたものであって、流通経路を流布するソフトウェアの不正使用の防止を促進できる新たなソフトウェア記憶媒体と、そのソフトウェア記憶媒体に記録されるソフトウェアを読み取るための新たなソフトウェア読取装置と、そのソフトウェア記憶媒体に記録されるソフトウェアの不正使用をチェックするための新たなソフトウェア管理システムとの提供を目的とするものである。

【0010】

【課題を解決するための手段】図1に本発明の原理構成を図示する。この本発明は、特に、流通経路を流布するソフトウェアがレンタル対象となるときに有効となるものである。

【0011】1は本発明により構成されるソフトウェア記憶媒体、2はメーカー等の出荷元に設置される出荷元装置、3はレンタル店等の中継先に設置される中継先装置、4はユーザ側に設置されるソフトウェア読取装置である。

【0012】ソフトウェア記憶媒体1としては、書換不可能記憶領域10と書換可能記憶領域11との混成からなる混成型記憶媒体が用いられる。出荷元装置2は、ソフトウェア記憶媒体1の書換不可能記憶領域10に、提供対象のソフトウェアの暗号情報を書き込む第1の書込手段20と、ソフトウェア記憶媒体1の書換可能記憶領域11に、提供対象のソフトウェアの保護情報をなす暗号ソフトウェア保護情報を書き込む第2の書込手段21とを備える。

【0013】この第2の書込手段21により書き込まれる暗号ソフトウェア保護情報は、第1の書込手段20により書き込まれる暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能時間と暗号情報からなり、先ず最初に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能時間とが鍵KYでもって暗号化されると、次に、その暗号情報が鍵KSTでもって暗号化されるというように、多重構成でもって暗号化されていく構成を採ることがある。ここで、使用可能時間については、中継先装置3で書き込まれる構成が採られることがあり、ソフトウェアが販売対象ではなくてレンタル対象となるときには、むしろその方が一般的である。

【0014】中継先装置3は、第2の書込手段21により書き込まれる暗号ソフトウェア保護情報の暗号構造を変更する暗号構造変更手段30と、中継先装置3の発行した使用可能時間を管理する時間データ管理手段31と、流通経路から回収されたソフトウェア記憶媒体1に記録されるソフトウェアの使用可能時間を集計する集計手段32と、時間データ管理手段31の管理値と集計手段32の集計値とを比較することによってソフトウェアの使用時間を特定する比較手段33とを備える。

【0015】この暗号構造変更手段30は、上述の例で説明するならば、鍵KSTでもって暗号ソフトウェア保護情報の最終段を復号すると、次に、その復号された暗号情報を鍵KSTとは異なる鍵KXでもって暗号化するような処理を実行していくことで、暗号ソフトウェア保護情報の暗号構造を変更する。また、この中継先装置3は、好ましくは、ソフトウェアの使用可能時間の集計をソフトウェア記憶媒体1の識別番号を単位にして実行していくことになる。

【0016】ソフトウェア読取装置4は、中継先から与えられるソフトウェア記憶媒体1の書換可能記憶領域11に記録される暗号ソフトウェア保護情報を復号することで、暗号ソフトウェアを復号するための鍵情報と、ソフトウェアの使用可能時間とを復号する第1の復号手段

(4)

特開平6-95871

5

4 0 と、第 1 の復号手段 4 0 の復号する鍵情報に従って、ソフトウェア記憶媒体 1 の書換不可能記憶領域 1 0 に記録される暗号ソフトウェアを復号する第 2 の復号手段 4 1 と、第 1 の復号手段 4 0 の復号する使用可能時間を経過時間に従って減算していくことで新たな使用可能時間を算出する算出手段 4 2 と、算出手段 4 2 の算出する新たな使用可能時間に従って、ソフトウェア記憶媒体 1 の記録する暗号ソフトウェア保護情報の使用可能時間を適時更新していく更新手段 4 3 と、第 1 の復号手段 4 0 の復号する使用可能時間か、算出手段 4 2 の算出する使用可能時間のいずれか一方がゼロ値を表示するときには、第 2 の復号手段 4 1 が復号処理を実行できないように制御する抑止手段 4 4 と、使用可能時間の減算値がゼロ値に達するとき新たな使用可能時間となる使用追加時間を設定して、本来の使用可能時間と識別可能となる態様に従いつつ、この新たな使用可能時間に従ってソフトウェア記憶媒体 1 の記録する暗号ソフトウェア保護情報の使用可能時間を更新する設定手段 4 5 とを備える。

【0017】

【作用】本発明では、流通経路を流布するソフトウェアを記録するためのソフトウェア記憶媒体 1 として、書換不可能記憶領域 1 0 と書換可能記憶領域 1 1 との混成からなる混成型記憶媒体を用意し、この混成型記憶媒体の書換不可能記憶領域 1 0 に、提供対象となるソフトウェアの暗号情報を記録する構成を採るとともに、書換可能記憶領域 1 1 に、暗号ソフトウェアを復号するための鍵情報とソフトウェアの使用可能時間との暗号情報を、暗号ソフトウェア保護情報として記録する構成を採る。

【0018】そして、このソフトウェア記憶媒体 1 のソフトウェアを読み取るユーザ側のソフトウェア読取装置 4 は、暗号ソフトウェア保護情報を復号することでソフトウェアの使用可能時間を得ると、この使用可能時間がゼロ値を表示していないときには、暗号ソフトウェア保護情報を復号することで得られる暗号ソフトウェア復号用の鍵情報を用いて暗号ソフトウェアを復号するとともに、経過時間に従って使用可能時間を減算して適時暗号ソフトウェア保護情報を更新し、一方、この使用可能時間がゼロ値を表示しているときには、暗号ソフトウェアの復号を実行しないよう処理する。そして、ソフトウェア記憶媒体 1 の使用可能時間の計時処理に入ったソフトウェア読取装置 4 は、読み取り指示のあるソフトウェア記憶媒体 1 の暗号ソフトウェア保護情報の使用可能時間がゼロ値を表示していないときであっても、そのソフトウェア記憶媒体 1 が取り外されている間にその使用可能時間がゼロ値に達している場合には、同様に、暗号ソフトウェアの復号を実行しないよう処理する。

【0019】この構成に従い、本発明では、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複製されるといったような不正使用にさらされることがあっても、ソフトウェ

6

アと一体的に記録されるソフトウェア保護情報の示す使用可能時間に従って、その使用可能時間以上のソフトウェアの使用を排除していくことになることから、その不正使用の幅値を大きく減ずることができるようになる。これから、流通経路を流布するソフトウェアの不正使用の防止を図れることになるのである。

【0020】そして、この構成において、中継先は、出荷元の出荷するソフトウェア記憶媒体 1 の暗号構造を変更してユーザ側に提供し、ユーザ側のソフトウェア読取装置 4 は、この変更された暗号構造を復号することでソフトウェアの復号処理を実行していく構成を採ると、出荷元と中継先との間での不正使用は意味をなさないことから、ソフトウェアの不正使用を積極的に防止することができるようになる。

【0021】更に、本発明では、中継先装置 3 は、流通経路から回収されたソフトウェア記憶媒体 1 に記録されるソフトウェアの使用可能時間の集計値を算出するとともに、この集計値と発行した使用可能時間との差分によりソフトウェアの使用時間を特定して、その使用時間に応じた使用料金を算出していくよう処理する。

【0022】この構成に従い、本発明では、貸し出したソフトウェアの使用時間を正確に特定できるとともに、ソフトウェアが不正復号されるようなことがあっても、どのソフトウェアがどれ位不正復号されたのかを特定できるようにするので、ソフトウェアの不正使用の実態も正確に把握できるようになるのである。

【0023】

【実施例】以下、実施例に従って本発明を詳細に説明する。図 2 に、本発明の適用される流通システムの一例を図示する。この図の流通システムは、保護対象のソフトウェアを出荷するメーカーと、メーカーの出荷するソフトウェアを貸し出すレンタル店と、レンタル店の貸し出すソフトウェアを購入するユーザとからなる。

【0024】このような流通システムに本発明を適用する場合、図 1 で説明した出荷元装置 2 はメーカーに設置され、中継先装置 3 はレンタル店に設置され、ソフトウェア読取装置 4 はユーザ側に設置されることになる。

【0025】図 1 で説明したように、本発明では、流通経路に置かれるソフトウェアを暗号化して、その暗号情報を混成型記憶媒体の書換不可能記憶領域 1 0 に記録するとともに、その暗号ソフトウェアの復号のための鍵情報と、そのソフトウェアの使用可能時間とからなるソフトウェア保護情報を暗号化して、その暗号情報をその混成型記憶媒体の書換可能記憶領域 1 1 に記録する構成を採ることで、ソフトウェアの不正使用の防止を実現するのである。

【0026】この記成型のソフトウェア記憶媒体 1 としては、例えば、書換不可能記憶領域 1 0 を光記憶媒体で構成するとともに、書換可能記憶領域 1 1 を磁気記憶媒体で構成するような記憶媒体が用いられる。なお、書換

(5)

特開平6-95871

7

不可能記憶領域10を書き換えが不可能であることに対応させて、以下ROM領域と称することがあり、また、書換可能記憶領域11を不揮発性ではあるが、書き換えが可能であることに対応させて、以下RAM領域と称することがある。

【0027】図3に、この記録構成を採る混成型のソフトウェア記憶媒体1に対する出荷段階での処理を司る出荷元装置2の装置構成の一実施例、図4及び図5に、このソフトウェア記憶媒体1に対する流通段階での処理を司る中継先装置3の装置構成の一実施例、図6及び図7に、このソフトウェア記憶媒体1に対する使用段階での処理を司るソフトウェア読取装置4の装置構成の一実施例を図示する。

【0028】次に、この図3ないし図7に従って、本発明のソフトウェア保護のメカニズムについて詳細に説明する。出荷元装置2は、図3に示すように、第1の暗号化手段200と、第2の暗号化手段202と、第3の暗号化手段204と、第1の鍵管理手段203と、第2の鍵管理手段204と、第3の鍵管理手段205と、入力手段206とを備える。

【0029】この装置構成を採るときにあって、ソフトウェア格納装置から出荷対象の平文のソフトウェアが与えられ、第1の暗号化手段200は、そのソフトウェアを第1の鍵管理手段203の管理する第1の鍵KUでもって暗号化することで、暗号ソフトウェア“E_{KU} (DATA)”を生成して、その暗号ソフトウェアを混成型のソフトウェア記憶媒体1のROM領域にスタンピングする。ここで、同時にスタンピングされる図中の“EOF”は、その暗号ソフトウェアの終了箇所を表示するものである。

【0030】次に、第2の暗号化手段201は、暗号ソフトウェア“E_{KU} (DATA)”の復号に必要となる第1の鍵KUを、第2の鍵管理手段204の管理する第2の鍵KVでもって暗号化することで、暗号ソフトウェア保護情報“E_{KV} (KU)”を生成する。続いて、第3の暗号化手段202は、入力手段206から入力されてくる各種レンタル情報と、第2の暗号化手段201の出力する暗号ソフトウェア保護情報“E_{KV} (KU)”とを、第3の鍵管理手段205の管理する第3の鍵KSでもって暗号化することで、暗号ソフトウェア保護情報“E_{KS} (レンタル情報/E_{KV} (KU))”を生成して、その暗号ソフトウェア保護情報を混成型のソフトウェア記憶媒体1のRAM領域に電氣的に書き込む。

【0031】そして、この図3では省略してあるが、出荷元装置2の図示しない書込手段は、暗号ソフトウェア保護情報のレンタル情報を、平文のままソフトウェア記憶媒体1のRAM領域にも電氣的に書き込んでいくよう処理することになる。ここで、入力手段206の与えるレンタル情報としては、販売なのかレンタルなのかを表示する選択コード（この場合にレンタルである）、ソフ

8

トウェア記憶媒体1の識別番号、ソフトウェア名といったものがある。

【0032】このようにして、出荷元装置2は、混成型のソフトウェア記憶媒体1のROM領域に、提供対象となるソフトウェアの暗号情報を記録し、更に、RAM領域に、その暗号ソフトウェアを復号するための鍵情報と、各種レンタル情報とからなるソフトウェア保護情報の暗号情報を記録していくよう処理するのである。

【0033】このような記録構成を採る混成型のソフトウェア記憶媒体1に対する流通段階での処理を司る中継先装置3は、メーカからソフトウェア記憶媒体1が供給されるときには、図4に示すように、復号手段300と、第1の暗号化手段301と、第2の暗号化手段302と、第3の鍵管理手段303と、第4の鍵管理手段304と、第1の交換鍵管理手段305と、時間管理手段306と、レンタル管理手段307と、入出力手段308とを備える構成を採る。

【0034】この装置構成を採るときにあって、メーカからソフトウェア記憶媒体1を受け取ると、復号手段300は、そのソフトウェア記憶媒体1のRAM領域に書き込まれている暗号ソフトウェア保護情報“E_{KS} (レンタル情報/E_{KV} (KU))”を、第3の鍵管理手段303の管理する第3の鍵KS_T (出荷元装置2の第3の鍵管理手段205の管理する鍵と同一のもの)でもって復号することで、暗号ソフトウェア保護情報“レンタル情報/E_{KV} (KU)”を生成する。

【0035】一方、時間管理手段306は、入出力手段308からソフトウェア記憶媒体1の使用可能時間 ΔT と、レンタル店発行のレンタル情報(レンタル店コード、ユーザコード等)とが入力されてくると、それらを第1の暗号化手段301に通知するとともに、復号手段300の復号したレンタル情報を受け取って、この受け取ったレンタル情報と入出力手段308からの入力情報とをレンタル管理手段307に登録する。そして、第2の暗号化手段302は、入出力手段308からソフトウェア記憶媒体1の識別番号が入力されてくると、その識別番号を第1の交換鍵管理手段305の管理する交換鍵でもって暗号化することで第4の鍵KVを得て、その第4の鍵KVを第4の鍵管理手段304に登録する。

【0036】復号手段300が復号処理を終了し、時間管理手段306が使用可能時間 ΔT 等を通知してくると、続いて、第1の暗号化手段301は、復号手段300の出力するレンタル情報・暗号ソフトウェア保護情報“E_{KV} (KU)”と、時間管理手段306の通知するレンタル情報・使用可能時間 ΔT とを、第4の鍵管理手段304の管理する第4の鍵KVでもって暗号化することで、暗号ソフトウェア保護情報“E_{KV} (レンタル情報/E_{KV} (KU))”を生成して、その暗号ソフトウェア保護情報を混成型のソフトウェア記憶媒体1のRAM領域に電氣的に書き込む。

(6)

時間平6-95871

9

10

【0037】そして、この図4では省略してあるが、中継先装置3の図示しない番送手段は、暗号ソフトウェア保護情報のレンタル店発行レンタル情報（使用可能時間 ΔT も含めることがある）を、平文のままソフトウェア記憶媒体1のRAM領域にも電氣的に書き込んでいくよう処理することになる。

【0038】このようにして、中継先装置3は、メーカからソフトウェア記憶媒体1が供給されると、供給されたソフトウェア記憶媒体1のRAM領域に書き込まれている暗号ソフトウェア保護情報“E_{K1}（レンタル情報／E_{K1}（KU））”に対して、使用可能時間 ΔT 及びレンタル情報を追加して、“E_{K1}（レンタル店発行レンタル情報／ ΔT ／E_{K1}（KU））”という別の暗号構造を持つものに書き換えていくよう処理するのである。

【0039】後述するように、ユーザ側に配置されるソフトウェア読取装置4は、鍵KXをもってソフトウェア記憶媒体1の暗号ソフトウェア保護情報を復号する構成を採ることで、ソフトウェア記憶媒体1のROM領域に書き込まれている暗号ソフトウェア“E_{K0}（DAT A）”を復号していく構成を採るものである。これから、このように、出荷元装置2が、鍵KSTで暗号ソフトウェア保護情報を生成するとともに、中継先装置3が、この暗号ソフトウェア保護情報を鍵KXで暗号化するものに書き換えていく構成を採ることで、メーカからレンタル店の流通経路の間で行われるソフトウェア記憶媒体1の不正使用を完全に排除することが実現できることになる。

【0040】図1で説明したように、本発明では、ソフトウェア記憶媒体1に記録される使用可能時間分、ソフトウェア記憶媒体1のROM領域に記憶されるソフトウェアの使用を許可する構成を採ることで、ソフトウェアの不正使用を排除していくことを実現するものである。この構成を実現するためには、下記の時間管理要件を充足する必要がある。

【0041】すなわち、レンタル店が単一のソフトウェア記憶媒体1を貸し出すときには、図8（a）に示すように、使用の有無にかかわらずに、貸し出し時点から規定のレンタル時間（この図では、14時間単位を想定している）が経過するときに、それ以降の使用を不可能にしておく必要がある。ここで、図中の1D1i（i=1～3）は、使用状態にあることを表している。また、レンタル店が複数のソフトウェア記憶媒体1を貸し出すときには、図8（b）に示すように、使用の有無にかかわらずに、貸し出し時点からそれぞれのレンタル時間が経過するときに、それ以降の使用を不可能にしておく必要がある。ここで、図中、1D1は14時間単位のレンタル時間、1D2は13時間単位のレンタル時間、1D3は11時間単位のレンタル時間、1D4は8時間単位のレンタル時間を想定している。

【0042】また、レンタル店が単一のソフトウェア記

憶媒体1を貸し出すときにあって、ユーザが異なる復号装置を用いながら使う場合にあって、図9に示すように、使用の有無にかかわらずに、貸し出し時点から規定のレンタル時間（この図では、14時間単位を想定している）が経過するときに、それ以降の使用を不可能にしておく必要がある。また、レンタル店が複数のソフトウェア記憶媒体1を貸し出すときにあって、ユーザが異なる復号装置を用いながら使う場合にあって、図10に示すように、使用の有無にかかわらずに、貸し出し時点から規定のレンタル時間が経過するときに、それ以降の使用を不可能にしておく必要がある。ここで、図中、1D1は14時間単位のレンタル時間、1D2は13時間単位のレンタル時間を想定している。

【0043】このようなソフトウェアのレンタル使用の時間管理要件の充足の実現を司るソフトウェア読取装置4は、図6に示すように、第1の暗号化手段400と、第2の暗号化手段401と、第3の暗号化手段402と、第1の復号手段403と、第2の復号手段404と、第3の復号手段405と、状態表示メモリ406と、レンタル情報処理手段407と、出力手段408と、入出力手段409とを備える。

【0044】この装置構成を採るときにあって、ユーザがレンタル店から借り出したソフトウェア記憶媒体1の読み取りを指示すると、まず最初に、第1の暗号化手段400は、そのソフトウェア記憶媒体1のRAM領域に書き込まれている識別番号を、規定の変換鍵をもって暗号化することで、中継先装置3の第4の鍵管理手段304の管理する鍵と同一の鍵KXを生成する。

【0045】次に、第1の復号手段403は、ソフトウェア記憶媒体1のRAM領域に書き込まれている暗号ソフトウェア保護情報“E_{K1}（レンタル店発行レンタル情報／ ΔT ／E_{K1}（KU））”を、この第1の暗号化手段400の生成した鍵KXをもって復号することで、暗号ソフトウェア保護情報“レンタル店発行レンタル情報／ ΔT ／E_{K1}（KU）”を生成する。そして、その内のレンタル店発行レンタル情報と使用可能時間 ΔT とを状態表示メモリ406に書き込むとともに、暗号ソフトウェア保護情報“E_{K1}（KU）”を第2の復号手段404に通知する。ここで、状態表示メモリ406に書き込まれる使用可能時間 ΔT は、購入当初は、中継先装置3の入出力手段308の設定する値と一致する。

【0046】続いて、第2の復号手段404は、バッテリバックアップされた状態表示メモリ406に格納されている鍵KY（出荷元装置2の第2の鍵管理手段204の管理する鍵と同一のもの）を読み出し、第1の復号手段403の出力する暗号ソフトウェア保護情報“E_{K1}（KU）”を、この鍵KYをもって復号することで、ソフトウェア記憶媒体1に記録されている暗号ソフトウェア“E_{K0}（DATA）”の復号に必要となる鍵KUを生成する。そして、第2の復号手段404は、この復号

(7)

特開平6-95871

11

した鍵KUを状態表示メモリ406に書き込む。

【0047】一方、レンタル情報処理手段407は、状態表示メモリ406からソフトウェア記憶媒体1の識別番号と使用可能時間 ΔT とを読み込むと、後述する処理に従って、この使用可能時間 ΔT がゼロ値を表示するときは直ちに状態表示メモリ406に格納される鍵KUをクリアし、ゼロ値を表示しないときには、この使用可能時間 ΔT を経過時間に従って減算していくとともに、減算していく使用可能時間 $\Delta T'$ がゼロ値に達したか否かをチェックして、ゼロ値に達したときには状態表示メモリ406に格納される鍵KUをクリアし、ゼロ値に達しないときにはこのクリア処理を実行しないように処理していく。更に、ゼロ値を表示しないときであっても、ソフトウェア記憶媒体1が取り外されている間での計時処理に従って使用可能時間 $\Delta T'$ がゼロ値に達している場合には、状態表示メモリ406に格納される鍵KUをクリアしていく。

【0048】そして、第3の復号手段405は、状態表示メモリ406に格納される鍵KUを読み取ると、ソフトウェア記憶媒体1のROM領域に書き込まれている暗号ソフトウェア“Ex”(DATA)”を、この読み取った鍵KUでもって復号することで、提供対象となるソフトウェアを生成し、出力手段408は、この復号されたソフトウェアを図示しない出力機器に出力していく。このとき、第3の復号手段405は、状態表示メモリ406に格納される鍵KUがクリアされているときには、この復号処理を実行できない。

【0049】すなわち、ソフトウェア記憶媒体1に記録される使用可能時間 ΔT がゼロ値を表示しているか、その使用可能時間 ΔT が時間経過に従ってゼロ値に達するときは、ソフトウェア読取装置4は、ソフトウェア記憶媒体1に記録されたソフトウェアの使用を実行できないように動作していくのである。

【0050】そして、“EOF”に従ってソフトウェアの使用の終了が検出されると、第2の暗号化手段401は、状態表示メモリ406から読み出すレンタル店発行レンタル情報と、レンタル情報処理手段407の出力する新たな使用可能時間 $\Delta T'$ と、第1の復号手段403の出力する暗号ソフトウェア保護情報“Ex”(KU)”とを、与えられる鍵KXでもって暗号化することで、使用可能時間の減じられた新たな暗号ソフトウェア保護情報“Ex”(レンタル店発行レンタル情報/ $\Delta T'$ /Ex(KU))”を生成して、ソフトウェア記憶媒体1のRAM領域の暗号ソフトウェア保護情報をこの新たなものに書き換えていく。

【0051】一方、“EOF”に従ってソフトウェアの使用の終了が検出されると、第3の暗号化手段402は、状態表示メモリ406から読み出す装置パラメータ状態情報を規定の変換鍵でもって暗号化してから、ソフトウェア記憶媒体1のRAM領域にメンテナンス等のた

12

めに書き込んでいく。

【0052】次に、図7に従って、レンタル情報処理手段407の実行する時間管理処理について説明する。レンタル情報処理手段407は、この時間管理処理を実行するために、図7に示すように、CPU410と、1Dテーブル411と、バッテリバックアップされたサイクリックカウンタ412と、減算器413と、比較器414と、データバス415と、コントロールバス416と、インタフェース417、418と、セクタ419とを備える。

【0053】この装置構成を採るときにあって、ユーザがレンタル店から借り出したソフトウェア記憶媒体1の読み取りを指示すると、CPU410は、状態表示メモリ406から与えられるそのソフトウェア記憶媒体1の識別番号1Dと使用可能時間 ΔT とを1Dテーブル411に登録する。ここで、1Dテーブル411のエンtriは、ソフトウェア記憶媒体1がソフトウェア読取装置4から取り外されることがあっても、そのまま保持されることになるので、CPU410は、前に読み出し要求のあったソフトウェア媒体1については、この1Dテーブル411への登録処理を実行しない。

【0054】続いて、CPU410は、読み取り指示のあったソフトウェア記憶媒体1の使用可能時間 ΔT が1Dテーブル411に登録されていない場合には、比較器414に従って、新たに登録した使用可能時間 ΔT がゼロ値を表示しているか否かを判断して、ゼロ値を表示しているときには、状態表示メモリ406に格納される鍵KUのクリア処理を指示していくことで、第3の復号手段405の実行する復号処理を抑制していく。また、読み取り指示のあったソフトウェア記憶媒体1が1Dテーブル411に登録されているときには、1Dテーブル411の管理データに従って、そのソフトウェア記憶媒体1の使用可能時間 ΔT がゼロ値を表示しているか否かを判断して、ゼロ値を表示しているときには、状態表示メモリ406に格納される鍵KUのクリア処理を指示していくことで、第3の復号手段405の実行する復号処理を抑制していく。この抑制処理に従って、読み取りの指示されたソフトウェア記憶媒体1の使用可能時間 ΔT が残されていないときには、そのソフトウェア記憶媒体1の使用が禁止されていくことになる。

【0055】一方、バッテリバックアップされたサイクリックカウンタ412は、規定の経過時間に達すると、CPU410に対して割り込みを通知していくことで、一定時間経過毎にCPU410に対して割り込みを通知していく。この割り込みの通知があると、減算器413は、1Dテーブル411から使用可能時間 ΔT を順次読み出し、その使用可能時間 ΔT に対して割り込みカウンタ412の検出する規定経過時間分減算して、その減算値に従って1Dテーブル411の使用可能時間 ΔT を新たなものに更新していくとともに、比較器414は、減

(8)

特開平6-95871

13

14

算器413の減算処理に従って更新されていく使用可能時間 ΔT がゼロ値に達するときには、1Dテーブル411の対応するエントリの無効フラグに無効データであることを登録していく。

【0056】続いて、CPU410は、この割込処理が終了すると、使用中のソフトウェア記憶媒体1の使用可能時間 ΔT がゼロ値に達することで無効データとなったか否かを判断して、無効データとなった場合には、状態表示メモリ406に格納される鍵KUのクリア処理を指示していくことで、第3の復号手段405の実行する復号処理を抑止していく。この抑止処理に従って、使用可能時間 ΔT が無くなるときには、読み取り中のソフトウェア記憶媒体1の使用が禁止されていくことになる。そして、CPU410は、“EOF”に従ってソフトウェアの使用の終了が検出されると、1Dテーブル411から使用の終了したソフトウェア記憶媒体1の使用可能時間 $\Delta T'$ を読み出し、第2の暗号化手段401に通知していくことで、暗号ソフトウェア保護情報“E_K(レンタル店発行レンタル情報/ ΔT /E_K(KU))”の生成を実現していくとともに、その使用可能時間 $\Delta T'$ をソフトウェア記憶媒体1のRAM領域に書き込んでいく。

【0057】このようにして、レンタル情報処理手段407は、状態表示メモリ406からソフトウェア記憶媒体1の識別番号と使用可能時間 ΔT とを読み込むと、この使用可能時間 ΔT がゼロ値を表示するときには直ちに状態表示メモリ406に格納される鍵KUをクリアし、ゼロ値を表示しないときには、この使用可能時間 ΔT を経過時間に従って減算していくとともに、減算していく使用可能時間 $\Delta T'$ がゼロ値に達したか否かをチェックして、ゼロ値に達したときには状態表示メモリ406に格納される鍵KUをクリアし、更に、ゼロ値を表示しないときであっても、ソフトウェア記憶媒体1が取り外されている間に使用可能時間 $\Delta T'$ がゼロ値に達している場合には、状態表示メモリ406に格納される鍵KUをクリアしていく。そして、ソフトウェアの使用の終了が検出されると、減算した使用可能時間 $\Delta T'$ を第2の暗号化手段401に通知していくよう処理するのである。

【0058】なお、レンタル情報処理手段407は、上述のように、使用可能時間 ΔT の残されていないソフトウェア記憶媒体1に対して、直ちにその使用を禁止していくのではなくて、使用可能時間の追加を認めていく構成を採ることも可能である。すなわち、入出力手段409を介して、ユーザに対して、使用可能時間の追加を要求するか否かを問い合わせ、追加要求があるときには、ユーザに対して、追加要求のあるソフトウェア記憶媒体1の識別番号と追加時間とを入力させて、その追加時間を1Dテーブル11に登録(無効フラグも解除する)していくよう処理するのである。このとき、ソフトウェア読取装置4は、ソフトウェア記憶媒体1に登録す

る使用可能時間 ΔT については、後述する使用可能時間集計処理を正確に実現していくために、本来の使用可能時間 ΔT と識別可能となる態様に従いつつ、この新たな使用可能時間 ΔT を記録していくよう処理することになる。

【0059】このようにして、ソフトウェア読取装置4は、図6及び図7の構成に従って、ソフトウェア記憶媒体1に記録される暗号ソフトウェア保護情報を復号することでソフトウェアの使用可能時間を得ると、この使用可能時間がゼロ値を表示していないときには、暗号ソフトウェア保護情報の復号により得られる鍵情報を用いて暗号ソフトウェアを復号してユーザに提供していくとともに、経過時間に従って使用可能時間を減算してソフトウェア記憶媒体1の暗号ソフトウェア保護情報を適時更新し、一方、この使用可能時間がゼロ値を表示しているときには、暗号ソフトウェアの復号を実行しないよう処理する。

【0060】そして、ソフトウェア記憶媒体1の使用可能時間の計時処理に入ったソフトウェア読取装置4は、読み取り指示のあるソフトウェア記憶媒体1の暗号ソフトウェア保護情報の使用可能時間がゼロ値を表示していないときであっても、そのソフトウェア記憶媒体1が取り外されている間にその使用可能時間がゼロ値に達している場合には、同様に、暗号ソフトウェアの復号を実行しないよう処理するのである。

【0061】この構成に従い、本発明では、流送段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複写されといったような不正使用にさらされることがあっても、ソフトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能時間に従って、その使用可能時間以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減ずることができるようになって、不正使用の防止を図れることになる。

【0062】一方、レンタル店に設置される中継先装置3は、この使用形態を採るソフトウェア記憶媒体1のソフトウェアの使用形態も管理することになる。すなわち、中継先装置3は、ユーザから貸し出し時間のオーダーによりソフトウェア記憶媒体1が回収されるときには、図5に示すように、復号手段300と、第1の暗号化手段301と、第2の暗号化手段302と、第4の鍵管理手段304と、第1の変換鍵管理手段305と、時間管理手段306と、レンタル管理簿307と、入出力手段308と、第3の暗号化手段309と、第2の変換鍵管理手段310と、第4の鍵管理手段311と、モデム手段312とを備える構成を採る。

【0063】この装置構成を採るときにあつて、直接あるいはモデム手段312を介して、ユーザからソフトウェア記憶媒体1を受け取ると、まず最初に、第3の暗号化手段309は、入出力手段308から与えられる識別

(9)

特開平6-95871

15

番号を、第2の変換鍵管理手段310の管理する変換鍵でもって暗号化することで第4の鍵KX(図4で説明した第4の鍵管理手段304の管理する鍵と同一のもの)を得て、その第4の鍵KXを第4の鍵管理手段311に登録する。

【0064】次に、復号手段300は、ソフトウェア記憶媒体1のRAM領域に書き込まれている暗号ソフトウェア保護情報“E_{K1}(レンタル店発行レンタル情報/ΔT/E_{K1}(KU))”を、この第4の鍵管理手段304の管理する鍵KXでもって復号することで、暗号ソフトウェア保護情報“レンタル店発行レンタル情報/ΔT/E_{K1}(KU)”を生成する。そして、その内のレンタル店発行レンタル情報と使用可能時間ΔTとを時間管理手段306に通知するとともに、その暗号ソフトウェア保護情報“レンタル店発行レンタル情報/ΔT/E_{K1}(KU)”を第1の暗号化手段301に通知する。

【0065】一方、第2の暗号化手段302は、入力手段308からソフトウェア記憶媒体1の識別番号が入力されてくると、その識別番号を第1の変換鍵管理手段305の管理する変換鍵でもって暗号化することで第4の鍵KX(図4で説明した第4の鍵管理手段304の管理する鍵と同一のもの)を得て、その第4の鍵KXを第4の鍵管理手段304に登録する。そして、第1の暗号化手段301は、復号手段300が復号処理を終了すると、復号手段300の出力する暗号ソフトウェア保護情報“レンタル店発行レンタル情報/ΔT/E_{K1}(KU)”を、第4の鍵管理手段304の管理する第4の鍵KXでもって暗号化することで、暗号ソフトウェア保護情報“E_{K1}(レンタル店発行レンタル情報/ΔT/E_{K1}(KU))”を生成して、その暗号ソフトウェア保護情報を混成型のソフトウェア記憶媒体1のRAM領域に電氣的に書き込む。

【0066】このようにして、中継装置3は、ユーザからソフトウェア記憶媒体1が回収されると、そのソフトウェア記憶媒体1に記録されるレンタル店発行レンタル情報及び使用可能時間ΔTとを時間管理手段306に通知していくよう処理するのである。

【0067】中継装置3の時間管理手段306は、このレンタル店発行レンタル情報及び使用可能時間ΔTを収集すると、それらの情報をレンタル管理簿307に登録するとともに、収集した使用可能時間ΔTと、レンタル管理簿307に登録されている貸し出し時の使用可能時間ΔTとからソフトウェアの使用料を計算する。この算出結果を受けて、レンタル店は、ユーザに対してレンタル料を要求していくことになる。そして、続いて、回収されたソフトウェア記憶媒体1の使用可能時間ΔTをゼロ値に設定してから、陳列棚に並べて再びユーザに貸し出ししていくことになる。

【0068】更に、この時間集計手段306は、レンタル管理簿307の管理データの集計処理を実行すること

16

で、ソフトウェアの不正使用をチェックしていく処理を実行する。すなわち、レンタル管理簿307に管理される使用前の使用可能時間をソフトウェア記憶媒体1の識別番号を単位に特定する。そして、レンタル料の算出に用いた使用時間をソフトウェア記憶媒体1の識別番号を単位に集計して、この集計値が否定した貸し出し時点での使用可能時間を上回っているかをチェックしていくのである。

【0069】この構成に従い、本発明では、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。そして、この構成にあって、ソフトウェア記憶媒体1のレンタル先ユーザ名が特定できるようになっていると、どのユーザが不正複製等の不正使用をしたのかも特定可能となるのである。

【0070】図示実施例について説明したが、本発明はこれに限定されるものではない。例えば、実施例では、ソフトウェアの使用可能時間の初期値を流通途中のレンタル店で記録していく構成を開示したが、本発明はこれに限られることなく、出荷元で記録するようにしてもよいのである。また、実施例では、ソフトウェア記憶媒体1を貸し出す利用形態のもので開示したが、本発明はこれに限られることなく、販売する形態のものであってもよいのである。

【0071】

【発明の効果】以上説明したように、本発明によれば、流通段階で、ソフトウェアが不正に横流しされたり、万引きされたり、持ち逃げされたり、不正に複製されるといったような不正使用にさらされることがあっても、ソフトウェアと一体的に記録されるソフトウェア保護情報の示す使用可能時間に従って、その使用可能時間以上のソフトウェアの使用を排除していくことになることから、その不正使用の価値を大きく減らすことができるようになる。これから、流通経路を流布するソフトウェアの不正使用の防止を図れることになる。しかも、出荷元と中継先との間での不正使用は完全に排除できることになる。

【0072】そして、本発明によれば、流通段階で、どのソフトウェアがどれ位不正使用されたのかを特定できるようになるので、ソフトウェアの不正使用の実態を正確に把握できるようになる。しかも、この構成にあって、ソフトウェアの流通先を記録しておくことが可能であるならば、誰が不正複製等の不正使用をしたのかも特定可能となるのである。

【図面の簡単な説明】

【図1】本発明の原理構成図である

【図2】本発明の適用される流通システムの一例である。

【図3】出荷元装置の装置構成の実施例である。

(10)

特開平6-95871

17

【図4】中継先装置の装置構成の一実施例である。

【図5】中継先装置の装置構成の一実施例である。

【図6】ソフトウェア読取装置の装置構成の一実施例である。

【図7】ソフトウェア読取装置の装置構成の一実施例である。

【図8】時間管理要件の説明図である。

【図9】時間管理要件の説明図である。

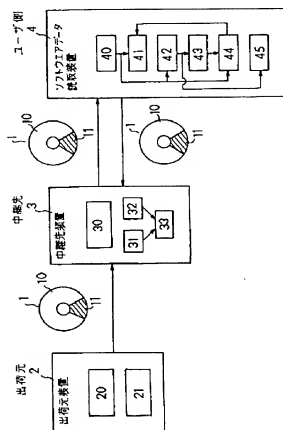
【図10】時間管理要件の説明図である。

【符号の説明】

- 1 ソフトウェア記憶媒体
- 2 出荷元装置
- 3 中継先装置
- 4 ソフトウェア読取装置

【図1】

本発明の原理構成図



18

10 帯換不可能記憶領域

11 帯換可能記憶領域

20 第1の帯込手段

21 第2の帯込手段

30 暗号構造変更手段

31 時間データ管理手段

32 集計手段

33 比較手段

40 第1の復号手段

10 41 第2の復号手段

42 算出手段

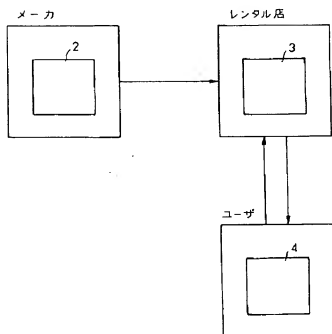
43 更新手段

44 抑止手段

45 設定手段

【図2】

本発明の適用される流通システムの一例

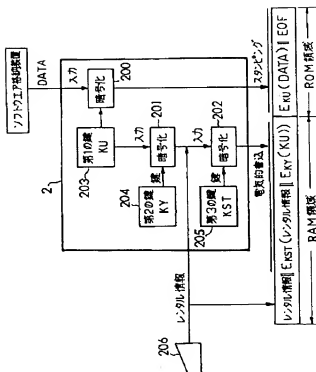


(11)

特開平6-95871

【図3】

出荷元装置の装置構成の一実施例



【図3】

時間順履歴データの説明図

